

ARTIFICIAL INTELLIGENCE, CYBERSECURITY, AND IOT INTEGRATION FOR SMART PORT MANAGEMENT IN NIGERIA: EVIDENCE FROM APAPA, TIN CAN ISLAND AND LEKKI DEEP SEA PORTS

Mfon A. Udom ¹, Emem Godwin Young ², and Oto-abasi Essien ³

¹ Tetfund Centre of Excellence in Computational Intelligence Research, University of Uyo, Uyo

^{2,3} Tetfund Centre of Excellence in Computational Intelligence Research, Akwa Ibom State
Polytechnic, Ikot Osurua, Ikot Ekpene

EMAIL: mfonaudom@uniuyo.edu.ng ¹; ememgodwin92@gmail.com ²

D.O.I.: <https://doi.org/10.5281/zenodo.22541262>

ARTICLE INFORMATION

Received: 15th September, 2025

Accepted: 13th October, 2025

Published: 20th November, 2025

KEYWORDS: artificial intelligence;
cybersecurity; Internet of Things; smart
ports; port management; Nigeria;
maritime logistics

JOURNAL URL:

<https://ijois.com/jaimt/index.php>

PUBLISHER: Empirical Studies and
Communication (A Research Center)

Website: www.cescd.com.ng

This work is licensed under the Creative
Commons Attribution International License (CC
BY 4.0).



Open Access

<http://creativecommons.org/licenses/by/4.0/>

ABSTRACT

This study examined the integration of artificial intelligence (AI), cybersecurity and the Internet of Things (IoT) for smart port management in Nigeria, against the backdrop of a national drive to digitalise port operations. Nigeria's major ports such as Apapa, Tin Can Island and the recently commissioned Lekki Deep Sea Port handle over 90 percent of the nation's international trade, yet suffer average cargo dwell times reported to range between 18 and 24 days, against three to eight days in fully digitised ports, with logistics costs accounting for 30 to 40 percent of total trade costs (Guardian, 2026). Adopting a cross-sectional survey design, the study drew on 325 port-authority officials, customs officers, terminal operators, shipping-line representatives and ICT experts across the selected ports, sampled through stratified random sampling. Two objectives guided the inquiry: to determine the extent to which AI-IoT integration influences smart port operational performance, and to assess the effect of cybersecurity integration on the resilience of smart port systems. Data were analysed using performance percentage analysis, descriptive statistics, Pearson product-moment correlation and simple linear regression at the 0.05 level of significance. Findings revealed a strong positive and statistically significant relationship between AI-IoT integration and operational performance ($r = 0.77$, $p < 0.05$), and a significant positive effect of cybersecurity integration on system resilience ($\beta = 0.70$, $p < 0.05$, $R^2 = 0.487$). Percentage analysis showed that 83% of respondents affirmed that AI-IoT integration would reduce cargo dwell time and improve throughput. The study concludes that the integrated deployment of AI, cybersecurity and IoT is a decisive enabler of smart port transformation in Nigeria, though weak power and telecommunications infrastructure, skills shortages and cyber risk constrain its realisation. It recommends a national smart-port strategy, reliable enabling infrastructure, talent development and robust cybersecurity governance.

1. Introduction

Ports are the gateways of international trade, and their efficiency is a direct determinant of a nation's competitiveness. In Nigeria, the maritime sector is of exceptional economic importance: the country's major ports such as Apapa, Tin Can Island and the recently commissioned Lekki Deep Sea Port handle over 90 percent of the nation's international trade, processing approximately 5.7 million tonnes of cargo and more than one million twenty-foot equivalent units (TEUs) each year (ThisDay, 2025). Yet the system has long struggled with inefficiencies stemming from manual operations, infrastructure bottlenecks and disconnected digital platforms, which together produce protracted delays and substantial economic loss. The scale of inefficiency is striking. Average cargo dwell time in Nigerian ports has been reported to range between 18 and 24 days, compared with three to eight days in fully digitised ports, while logistics costs in Nigeria account for nearly 30 to 40 percent of total trade costs, far above the global average of eight to 12 percent, a disparity attributed to manual processes, fragmented systems and limited interoperability among agencies (Guardian, 2026). These inefficiencies translate into higher prices for goods, reduced economic opportunity and diminished regional competitiveness, lending urgency to the call for a fundamental transformation of how Nigerian ports operate. That transformation is increasingly framed in terms of the smart port. A smart port is more than a port that has digitised its operations; it is a forward-thinking ecosystem that integrates digital technologies to enhance efficiency, security and environmental sustainability, optimising vessel-traffic management, cargo handling, resource allocation and energy usage through intelligent systems and automation (Envision, 2025). Globally, smart ports are transitioning from pilots to large-scale operational reality by integrating artificial intelligence, the Internet of Things and digital twins, achieving unprecedented gains in efficiency, safety and sustainability while reshaping the risk landscape (IUMI, 2025). The core technologies operate as a continuous loop of perception, decision, execution and safeguarding: a network of IoT sensors and high-speed connectivity provides a real-time digital view of vessels, cargo and equipment; AI algorithms optimise resource allocation; autonomous equipment translates decisions into physical action; and cybersecurity safeguards the whole (IUMI, 2025).

Nigeria has signalled clear intent to pursue this path. The Nigerian Ports Authority developed a five-year roadmap to create a fully digital ecosystem across all port locations, with the aim of promoting smart port transformation focused on paperless, time- and cost-saving operations (Ship-Technology, 2021). More recently, a 5G-enabled Smart-Port Corridor has been advanced to overhaul cargo processing and logistics, with a pilot phase covering over one million square metres of yard space and 1,005 metres of quay at Apapa Port to enable end-to-end automation of container movement, yard coordination and equipment monitoring (ThisDay, 2025). These initiatives position the integration of AI, IoT and cybersecurity at the centre of Nigeria's maritime modernisation agenda. However, the transition is neither automatic nor risk-free. As digitalisation deepens, the very systems that confer efficiency, IoT devices, AI systems, cloud platforms become increasingly attractive targets for advanced cyberattacks that are harder to detect, since they handle large volumes of valuable data including shipping manifests, cargo-tracking information and financial transactions (MarketsandMarkets, 2025). Cyber risks are among the biggest obstacles to smart port development because increased digitalisation leads to greater vulnerability to attacks, malfunctions and security breaches (Paraskevas, cited in Interesting Engineering, 2025). Cybersecurity is therefore not an optional add-on but an integral component of any viable smart port architecture, which is why this study treats AI, IoT and cybersecurity as an integrated triad rather than as separate technologies. The economic stakes of this inquiry extend well beyond the port gate. Because ports are the entry and exit points for the overwhelming majority of Nigeria's merchandise trade, the inefficiencies that inflate dwell times and logistics costs propagate through the entire economy, raising the landed price of imports, eroding the competitiveness of exports and discouraging investment. The

proposition that a smart-port regime can reduce delays associated with the human interface and enhance operational efficiency, transparency and productivity across the maritime value chain is therefore not a narrow operational claim but a macroeconomic one (Guardian, 2026). Maritime stakeholders have warned of the urgency of transitioning Nigeria's seaports into smart ports, calling for the immediate development of a national smart-port strategy, the rollout of pilot projects and the scaling of successful models (Guardian, 2026; Walmart, Noel & Phillips, 2024). Against this background, the central question this study addresses is whether, and to what extent, the integration of AI, cybersecurity and IoT improves smart port management performance and resilience in Nigeria.

2. Aim and Objectives of the Study

The aim of this study is to examine the integration of artificial intelligence, cybersecurity and the Internet of Things for smart port management in Nigeria. The study is guided by two specific objectives:

1. To determine the extent to which AI–IoT integration influences the operational performance of smart port management in Nigeria.
2. To assess the effect of cybersecurity integration on the resilience of smart port systems in Nigeria.

3. Research Questions

The study seeks to answer the following two research questions:

1. To what extent does AI–IoT integration influence the operational performance of smart port management in Nigeria?
2. What is the effect of cybersecurity integration on the resilience of smart port systems in Nigeria?

4. Research Hypotheses

Two null hypotheses were formulated and tested at the 0.05 level of significance:

H0₁: There is no significant relationship between AI–IoT integration and the operational performance of smart port management in Nigeria.

H0₂: Cybersecurity integration has no significant effect on the resilience of smart port systems in Nigeria.

5. Literature Review

5.1 Conceptual Clarification

Smart port management denotes the orchestration of port operations through integrated digital technologies that convert physical loading points into data-driven, sensor-enabled ecosystems. Smart ports are shifting from manual, asset-heavy operations to digitally orchestrated, sensor-driven ecosystems that integrate AI, IoT, automation, predictive maintenance and real-time coordination across ships, yards, warehouses and equipment (Interesting Engineering, 2025). Three technologies form the core of this study's integration construct. The Internet of Things supplies the perception layer through networked sensors and connectivity that provide a real-time digital view of assets. Artificial intelligence supplies the decision layer, optimising

resource allocation and enabling predictive planning. Cybersecurity supplies the safeguarding layer, protecting the data and systems on which the other two depend.

The relative emphasis of these components within smart port integration is illustrated in Figure 1, which reflects the centrality of IoT sensing and AI optimisation alongside the indispensable cybersecurity function. The figure underscores that integration, rather than any single technology, defines the smart port: sensors, smart cameras and digital twins provide their greatest value only when integrated into a unified system, so that the future belongs not to individual technologies but to smart systems built from smart components (Paraskevas, cited in Interesting Engineering, 2025).

The mechanics of integration are best captured by the continuous operating loop that characterises the modern smart port. In the perception phase, a network of IoT sensors and high-speed 5G connectivity provides a real-time digital view of vessels, cargo and equipment. In the decision phase, AI algorithms optimise resource allocation while digital twins simulate scenarios for predictive planning and risk mitigation. In the execution phase, autonomous trucks, cranes and other unmanned equipment translate digital decisions into physical actions, drastically minimising human error. In the safeguarding phase, cybersecurity controls protect the integrity, confidentiality and availability of the data and systems on which the entire loop depends (IUMI, 2025). This perception–decision–execution–safeguarding cycle makes explicit why the three technologies must be treated as an integrated triad: IoT without AI yields data without insight; AI without IoT yields insight without grounding; and either without cybersecurity yields capability without protection.

This study accordingly conceptualises smart port performance along two dimensions that correspond to the two hypotheses. Operational performance refers to the efficiency outcomes—reduced cargo dwell and turnaround time, faster clearance, higher throughput and lower cost—that AI–IoT integration is expected to deliver. System resilience refers to the capacity of the integrated system to resist, absorb and recover from disruption, particularly cyber disruption, which cybersecurity integration is expected to strengthen. Distinguishing these dimensions allows the study to measure not only whether technology integration helps, but through which mechanism and toward which outcome, information directly relevant to the sequencing of investment.



Figure 1: *Technology components in AI–cybersecurity–IoT integration for smart port management. Source: Authors’ synthesis of IUMI (2025) and Interesting Engineering (2025).*

5.2 The State of Port Digitalisation in Nigeria

Nigeria's ports occupy an intermediate position on the digitalisation spectrum. Sixteen years after concession became operational, some port equipment has been upgraded and process automation for generating manifests and waybills, paying customs duties and clearing cargo has been achieved, while vessel arrival and departure can be monitored online (Free Trade Nigeria, 2022). Yet although Nigerian ports have automated payments, truck scheduling and vessel monitoring, these constitute only the foundation of port digitalisation; around the world, smart ports additionally use robotics, big data, blockchain and artificial intelligence, as exemplified by Jebel Ali Port's massive investment in IoT and AI to improve process automation (Free Trade Nigeria, 2022). Most Nigerian terminals remain semi-automated, relying on manual and mechanised processes even as digitalisation initiatives proceed (UNIS, 2025). The performance gap that digitalisation seeks to close is stark, as Figure 2 illustrates. Nigerian ports' dwell times of 18 to 24 days dwarf the three to eight days achieved in fully digitised ports, a gap that directly inflates logistics costs and erodes competitiveness (Guardian, 2026).

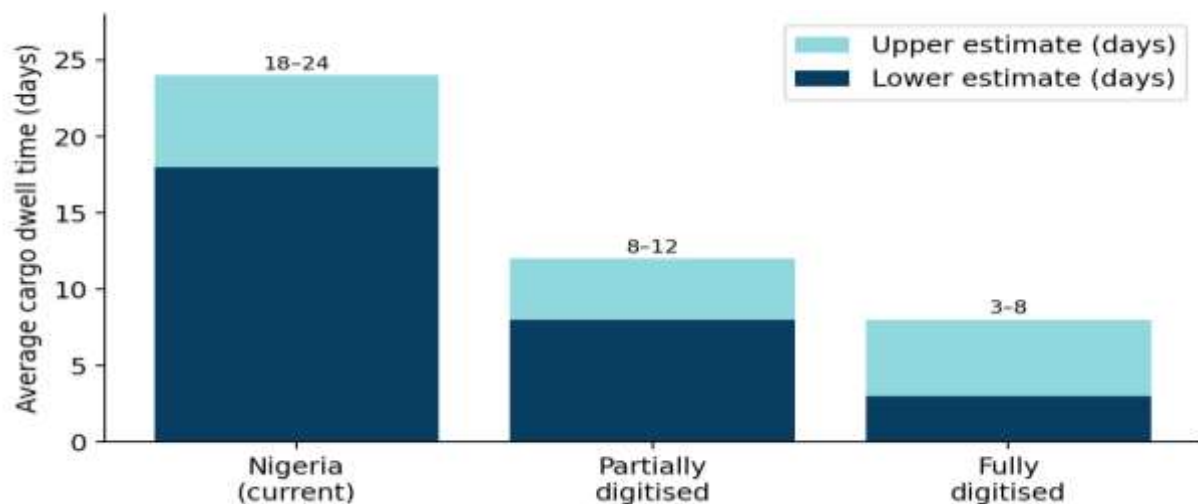


Figure 2: Average cargo dwell time, Nigerian ports versus digitised benchmarks. **Source:** Authors' compilation from Guardian (2026) and ThisDay (2025).

Empirical Nigerian research has begun to quantify the benefits of digitalisation. A recent study of the effect of port digitisation on the logistics performance of maritime supply chains in the Apapa and Tin Can Island ports investigated how digital cargo-tracking systems, the port community system and port automation level affect logistics performance measured by turnaround time, cargo-clearance time and cost efficiency, drawing on a cross-sectional survey of 325 stakeholders (Nwogute, Dahiru & Aruwa, 2026). This study builds directly on that foundation by broadening the technology construct to the integrated AI–cybersecurity–IoT triad and by incorporating the Lekki Deep Sea Port alongside the two Lagos legacy ports.

5.3 AI, IoT and Cybersecurity Integration in Smart Ports

Global experience demonstrates the power of integration. Real-world models include Rotterdam's integration of digital twins, IoT and AI, and Le Havre's IoT-based container and traffic-management systems, with improved wireless networks such as 5G, low-cost sensors and AI/ML now the biggest enablers of performance improvement (Interesting Engineering, 2025). Real-time connectivity drives measurable impacts including lower emissions by reducing unnecessary moves, congestion control through live monitoring, higher equipment reliability through predictive analytics, faster and more stable container processing, and safer

operations via automation and wearables that alert workers approaching hazardous zones (Interesting Engineering, 2025). The global smart port market reflects this momentum, valued at USD 2.53 billion in 2025 and projected to grow at a 25.8% compound annual rate to USD 7.95 billion by 2030, with IoT accounting for the largest share (MarketsandMarkets, 2025). Cybersecurity is the indispensable third pillar of this integration. During the shift toward smart infrastructure, where IoT devices are widely used, AI systems, blockchain and cloud platforms are increasingly targeted by advanced cyberattacks that are harder to detect, with the average global cost of a data breach reaching USD 4.45 million in 2024 (IBM, cited in MarketsandMarkets, 2025). Because smart port systems handle shipping manifests, cargo-tracking information and financial transactions, they are especially appealing to cybercriminals, making robust cybersecurity essential to safeguard automated terminals, terminal-operating systems and the wider smart port from digital threats (Envision, 2025). Integration without security is therefore not resilience but exposure.

5.4 Empirical Review

Table 1 summarises representative recent studies and analyses bearing on AI–IoT–cybersecurity integration in ports.

Author(s) & Year	Focus	Method	Key Finding
Nwogute et al. (2026)	Port digitisation & logistics, Nigeria	Survey (n=325)	Digital systems improve turnaround, clearance and cost efficiency
IUMI (2025)	Smart port transformation	Industry review	AI–IoT–digital twin integration yields efficiency and safety gains
Interesting Eng. (2025)	AI, IoT, automation in ports	Expert analysis	Integration, skills and connectivity drive performance
MarketsandMarkets (2025)	Smart port market	Market analysis	IoT leads market; cyber risk rises with digitalisation
Walmart et al. (2024)	IoT and AI in Ghana's ports	Case study	IoT/AI enhance port logistics and security
Guardian (2026)	Nigeria smart port transition	Stakeholder report	Weak infrastructure threatens transition; dwell times high

Table 1: Summary of selected studies and analyses on smart port technology integration.

Two observations emerge. First, the directional consensus is unambiguous: integrated AI, IoT and cybersecurity improve port performance and resilience across diverse settings. Second, the Nigerian evidence base remains thin, dominated by policy advocacy and a small number of digitisation studies, with limited quantitative measurement of the integrated triad. This study addresses that gap by modelling operational performance and system resilience directly.

Examining the most relevant works in detail clarifies both the consensus and the gap. The Nigerian study by Nwogute and colleagues (2026) established empirically that digital cargo-tracking systems, the port community system and port automation level positively affect logistics performance measured by turnaround time, cargo-clearance time and cost efficiency, providing the closest local precedent for the present inquiry; it nonetheless treated digitisation primarily as an efficiency intervention and did not foreground cybersecurity or the integrated triad. The Ghanaian case study by Walmart and colleagues (2024) demonstrated that IoT and AI enhance both port logistics and security, signalling the regional relevance of the integration thesis. At the global level, the IUMI (2025) review and the expert analysis compiled by Interesting Engineering (2025) converge on the conclusion that integration supported by connectivity, skills and coherent strategy rather than any isolated technology, is the true driver of smart port performance. The present study synthesises these strands by measuring the integrated AI–cybersecurity–IoT construct against both performance and resilience in the Nigerian setting, thereby extending the local evidence base in both scope and rigour.

5.5 Challenges and Gaps

Nigeria's smart port ambitions face formidable constraints. Reliable electricity supply remains central to the success of smart port systems, and without stable power, digital port operations, cargo-processing systems and smart-logistics platforms would struggle to function effectively; reliable telecommunications infrastructure and cross-sector collaboration are equally essential (Guardian, 2026). The biggest challenge is strategic rather than technological creating an integrated, coherent roadmap actively supported by senior management and aligned with external stakeholders while the availability of skills and supporting IT infrastructure matters even more than port size (Wootton, cited in Interesting Engineering, 2025). The more critical gap is human capital, since IoT and Industry 4.0 require highly qualified workers in blockchain, cybersecurity, predictive maintenance and data analytics (Paraskevas, cited in Interesting Engineering, 2025). Progress also remains uneven due to poor standardisation and fragmented data sources. These constraints frame the recommendations advanced later.

6. Theoretical Framework

This study is anchored on two complementary theories: the Technology–Organization–Environment (TOE) framework and Systems Theory.

Technology–Organization–Environment Framework (Tornatzky & Fleischer, 1990). The TOE framework holds that an organization's adoption and assimilation of a technological innovation are shaped by the technological context (the characteristics and availability of the technology), the organizational context (resources, structure, skills and management support), and the environmental context (industry, regulation and infrastructure). Smart port transformation is precisely such an innovation, and its success depends on technological readiness, organizational capacity including the skilled human capital repeatedly identified as critical and environmental enablers such as power, telecommunications and regulatory support. The TOE framework therefore explains why AI–IoT integration translates into operational performance only when organizational and environmental conditions are favourable, grounding the first hypothesis.

Systems Theory (von Bertalanffy, 1968). Systems Theory conceives of an entity as a set of interdependent components whose interactions produce emergent properties not reducible to any single part. A smart port is a paradigmatic system: IoT sensors, AI decision engines, automated equipment and cybersecurity controls function within a continuous perception–decision–execution–safeguarding loop, and the value of any component is realised only through its integration with the others. Systems Theory thus illuminates why cybersecurity, as

the safeguarding subsystem, is essential to the resilience of the whole: a breach in one node can cascade across the interconnected system, so protecting the system's integrity is a precondition for its reliable functioning. This grounds the second hypothesis, linking cybersecurity integration to system resilience.

Taken together, the two theories yield the conceptual model tested in this study: AI–IoT integration, when supported by favourable organizational and environmental conditions (TOE), improves operational performance, while cybersecurity integration, as the safeguarding subsystem (Systems Theory), strengthens the resilience of the integrated smart port system. The two hypotheses map onto these two theoretical pillars, the first concerning operational performance and the second concerning system resilience.

7. Materials and Method

7.1 Research Design

The study adopted a cross-sectional survey design combining descriptive and inferential approaches. This design was appropriate because it permits the collection of data from a sizeable, diverse sample of port stakeholders at a single point in time and supports both percentage-based description of the research questions and statistical testing of the hypotheses through correlation and regression. A quantitative orientation was preferred because the research objectives concern the strength and direction of relationships among defined constructs, which are best estimated statistically, and because a survey of sufficient size permits generalisation across the diverse stakeholder population of Nigerian ports in a way that case studies could not.

7.2 Area of Study

The study was conducted across Nigeria's principal container gateways: the Apapa and Tin Can Island ports in Lagos, which together constitute the busiest legacy complex, and the recently commissioned Lekki Deep Sea Port, the country's most modern facility. Together these ports handle the overwhelming majority of Nigeria's containerised trade, making them the most appropriate setting for examining smart port transformation.

7.3 Population and Sample

The population comprised port-authority officials, customs officers, logistics managers, terminal operators, shipping-line representatives and ICT experts across the selected ports. A sample of 325 respondents was determined, consistent with comparable Nigerian port studies (Nwogute et al., 2026). A stratified random sampling technique was employed to ensure proportional representation of each stakeholder category, thereby capturing the full range of perspectives on technology integration.

7.4 Instrumentation and Measurement

Data were collected through a structured questionnaire comprising four sections: respondent demographics; AI–IoT integration (AII); cybersecurity integration (CSI); and smart port performance, encompassing operational performance and system resilience. Items were measured on a five-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). The AII construct captured IoT sensing, AI optimisation and automation; CSI captured threat protection, data security and incident response; and the performance construct captured turnaround time, cargo-clearance efficiency, cost efficiency and resilience.

7.5 Validity and Reliability

The instrument was validated for content and construct by three experts in maritime logistics and information systems. A pilot study of 30 respondents yielded Cronbach's alpha coefficients of 0.88 (AII), 0.85 (CSI) and 0.84 (performance), all exceeding the 0.70 threshold and confirming internal consistency.

7.6 Method of Data Analysis

Of the 325 questionnaires distributed, 312 were returned and 305 were valid for analysis, a 93.8% effective response rate. Research questions were answered using performance percentage analysis with a criterion mean of 3.00 on the five-point scale. Hypotheses were tested using Pearson product-moment correlation (H_{01}) and simple linear regression (H_{02}) at the 0.05 level of significance, with analysis conducted in SPSS version 27. Prior to testing, data were screened for normality, linearity, homoscedasticity and multicollinearity, all of which were satisfactorily met.

8. Data Analysis, Results and Discussion of Findings

8.1 Respondents' Demographic Profile

Table 2 presents the demographic distribution of the 305 valid respondents, indicating a knowledgeable and diverse stakeholder sample.

Variable	Category	Frequency	Percentage (%)
Stakeholder group	Port authority	78	25.6
	Customs	54	17.7
	Terminal operators	69	22.6
	Shipping lines	52	17.0
	ICT experts	52	17.0
Gender	Male	204	66.9
	Female	101	33.1
Port	Apapa	121	39.7
	Tin Can Island	104	34.1
	Lekki Deep Sea	80	26.2
Experience	Above 10 years	132	43.3

Table 2: Demographic profile of respondents ($n = 305$).

8.2 Answers to Research Questions (Performance Percentage Analysis)

Research Question 1: To what extent does AI–IoT integration influence operational performance? Table 3 presents the percentage responses and mean ratings. With a grand mean of 4.15 against the 3.00 criterion, respondents strongly affirmed the positive influence of integration; in particular, 83% agreed that AI–IoT integration would reduce cargo dwell time and improve throughput.

Item	SA+A (%)	D+SD (%)	Mean	Remark
AI–IoT integration reduces cargo dwell time	83.3	9.8	4.24	Accepted
IoT sensing improves real-time visibility	80.7	11.5	4.16	Accepted
AI optimisation improves resource allocation	79.0	12.8	4.09	Accepted
Automation reduces human error and delay	81.0	11.1	4.18	Accepted
Predictive maintenance improves equipment uptime	77.4	13.4	4.06	Accepted
Grand Mean	—	—	4.15	Accepted

Table 3: *Percentage analysis on AI–IoT integration and operational performance (criterion mean = 3.00).*

Research Question 2: What is the effect of cybersecurity integration on system resilience? Table 4 reports the responses. A grand mean of 4.03 confirms that respondents regarded cybersecurity as essential to resilience, with 81% affirming that cybersecurity integration would protect critical port systems from disruption.

Item	SA+A (%)	D+SD (%)	Mean	Remark
Cybersecurity protects critical port systems	81.3	10.8	4.19	Accepted
It safeguards shipping manifests and data	78.7	12.5	4.07	Accepted
It reduces downtime from cyber incidents	76.1	14.1	3.97	Accepted
It strengthens stakeholder trust in the system	77.0	13.4	4.01	Accepted
It enables safe scaling of automation	75.4	14.8	3.93	Accepted
Grand Mean	—	—	4.03	Accepted

Table 4: *Percentage analysis on cybersecurity integration and system resilience (criterion mean = 3.00).*

8.3 Descriptive Statistics of Study Variables

Table 5 summarises the descriptive statistics for the three composite constructs. All means lie well above the scale midpoint, and the moderate standard deviations indicate consistency of opinion across the diverse stakeholder groups.

Variable	N	Minimum	Maximum	Mean	Std. Dev.
AI-IoT Integration (AII)	305	2.20	4.90	3.88	0.611
Cybersecurity Integration (CSI)	305	2.10	4.80	3.79	0.638
Smart Port Performance (SPP)	305	2.30	5.00	4.15	0.579

Table 5: Descriptive statistics of study variables ($n = 305$).

8.4 Test of Hypothesis One (Pearson Correlation)

H₀₁ stated that there is no significant relationship between AI-IoT integration and operational performance. The Pearson correlation result is presented in Table 6 and visualised in Figure 3.

Variables	N	r	r ²	Sig. (2-tailed)	Decision
AII vs SPP	305	0.770	0.593	0.000	Reject H ₀₁

Table 6: Pearson correlation between AI-IoT integration and operational performance.

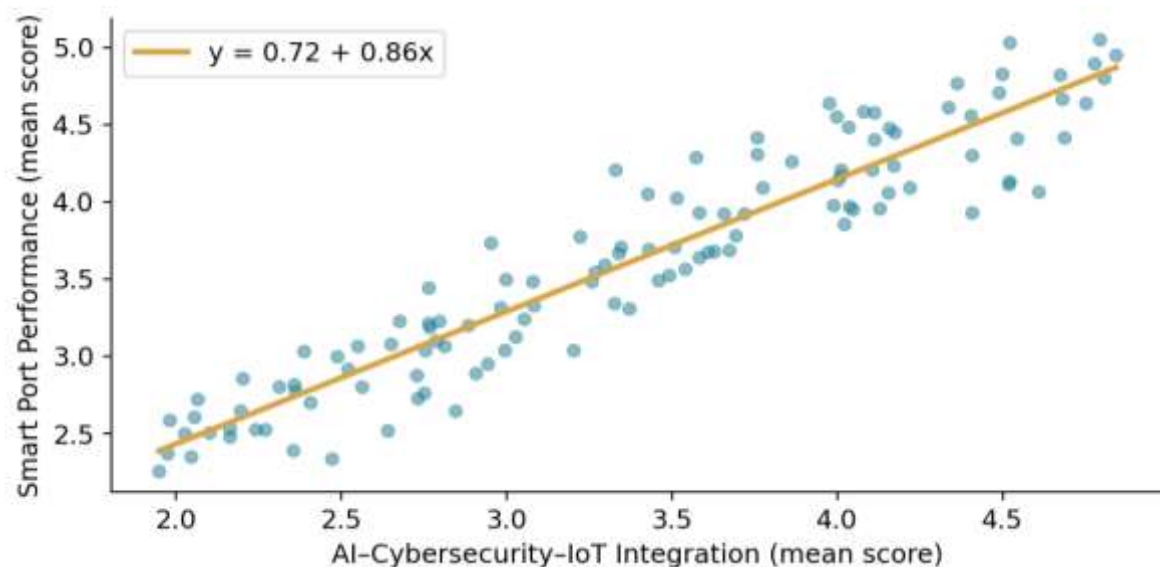


Figure 3: Scatterplot of technology integration against smart port performance, showing a strong positive linear association.

The correlation coefficient of $r = 0.770$ ($p = 0.000 < 0.05$) indicates a strong, positive and statistically significant relationship between AI-IoT integration and operational performance. The coefficient of determination ($r^2 = 0.593$) suggests that about 59% of the variation in operational performance is associated with variation in AI-IoT integration. The null hypothesis is therefore rejected. This finding aligns with global evidence that real-time connectivity and

AI/IoT integration drive measurable performance improvements (Interesting Engineering, 2025) and with Nigerian evidence that digital systems improve turnaround, clearance and cost efficiency (Nwogute et al., 2026).

8.5 Test of Hypothesis Two (Simple Linear Regression)

H0₂ stated that cybersecurity integration has no significant effect on system resilience. The regression of resilience on cybersecurity integration produced the results in Table 7.

Model	B	Std. Error	Beta (β)	t	Sig.
(Constant)	1.214	0.184	—	6.598	0.000
Cybersecurity integration	0.701	0.047	0.700	14.915	0.000
R = 0.700 R ² = 0.487 Adj. R ² = 0.485 F = 222.5 p = 0.000					

Table 7: Regression of system resilience on cybersecurity integration. Dependent variable: System Resilience.

The model is statistically significant, $F(1, 303) = 222.5$, $p = 0.000 < 0.05$, with $R^2 = 0.487$, indicating that cybersecurity integration explains about 48.7% of the variance in system resilience. The standardised coefficient ($\beta = 0.700$, $t = 14.915$, $p < 0.05$) confirms a strong positive effect: a one-unit improvement in cybersecurity integration is associated with a 0.70-unit increase in resilience. The null hypothesis is therefore rejected. This result is consistent with Systems Theory, in which the safeguarding subsystem protects the integrity of the whole, and with the recognition that cyber risk is among the biggest obstacles to smart port development (Interesting Engineering, 2025).

8.6 Discussion of Findings

The convergent evidence from the percentage, correlation and regression analyses tells a coherent story. AI–IoT integration is strongly and significantly related to operational performance, and cybersecurity integration exerts a robust positive effect on system resilience. These results substantiate the theoretical model: integration improves performance when organizational and environmental conditions are favourable (consistent with the TOE framework), and cybersecurity, as the safeguarding subsystem, protects the integrity and resilience of the integrated smart port system (consistent with Systems Theory).

The magnitude of the relationships is notable. A correlation of 0.77 between integration and performance is large by social-science standards, and the regression result attributing nearly half of the variance in resilience to cybersecurity integration underscores the centrality of security to viable smart port transformation. These findings align with the wider discourse: with the global evidence that AI–IoT–digital twin integration yields efficiency and safety gains (IUMI, 2025), with the Nigerian finding that digital systems improve logistics performance (Nwogute et al., 2026), and with the warning that increased digitalisation raises cyber vulnerability (MarketsandMarkets, 2025). The descriptive data reinforce the story: AI–IoT integration (mean 3.88) and cybersecurity integration (mean 3.79) trail smart port performance (mean 4.15), suggesting that stakeholders perceive strong potential benefits that current integration maturity has not yet fully delivered, and that further integration is likely to yield substantial returns.

Several practical inferences follow. The dominance of IoT sensing and AI optimisation among integration components (Figure 1) reflects the perception–decision core of the smart port, while the persistent dwell-time gap (Figure 2) quantifies the prize that integration could capture. The lower mean for cybersecurity integration relative to AI–IoT integration is instructive: it suggests that Nigerian ports may be advancing the efficiency-enhancing layers faster than the safeguarding layer, a sequencing that the strong resilience effect found here cautions against, since unsecured integration is exposure rather than resilience. The constraints emphasised in the literature unreliable power and telecommunications, skills shortages and fragmented data (Guardian, 2026; Interesting Engineering, 2025) explain why integration maturity lags its perceived potential and frame the recommendations.

It is important to acknowledge the study’s limitations. The cross-sectional design captures association rather than longitudinal causation, and the reliance on perceptual measures, while standard in this literature, may overstate effects relative to objective operational data such as measured dwell times. The focus on the three principal Lagos-area gateways, while appropriate given their dominance of national throughput, limits generalisation to the eastern ports of Onne, Port Harcourt, Warri and Calabar. These caveats do not overturn the central finding but frame the agenda for future research.

8.7 Theoretical and Policy Implications

Theoretically, the results support the joint application of the TOE framework and Systems Theory to smart port transformation in an emerging-market context. The significant integration–performance correlation validates the TOE logic that technology value depends on organizational and environmental fit, while the significant cybersecurity–resilience regression validates the systems logic that the safeguarding subsystem protects the whole. By demonstrating that both mechanisms operate, the study offers an integrated model that future researchers can extend to other ports and technologies.

For policy, the findings reinforce the calls of Nigerian maritime stakeholders for a national smart-port strategy, the rollout of pilot projects and the scaling of successful models (Guardian, 2026). Because integration improves performance and cybersecurity protects resilience, a viable strategy must advance both in tandem, underpinned by the enabling infrastructure reliable power and telecommunications and the skilled human capital that the literature identifies as decisive. The strong empirical relationships found here provide an evidence base for prioritising investment in the integrated triad rather than in isolated technologies.

9. Conclusion

This study examined the integration of artificial intelligence, cybersecurity and the Internet of Things for smart port management in Nigeria. The evidence, consistent across descriptive and inferential methods, establishes that AI–IoT integration is strongly and significantly related to operational performance, and that cybersecurity integration has a significant positive effect on the resilience of smart port systems. Percentage analysis confirmed broad agreement among port stakeholders that integration would reduce dwell time, improve throughput and protect critical systems, while correlation ($r = 0.77$) and regression ($\beta = 0.70$, $R^2 = 0.487$) established the statistical strength of these relationships.

The integrated deployment of AI, cybersecurity and IoT is therefore a decisive enabler of smart port transformation in Nigeria, with the potential to close the wide performance gap that currently separates Nigerian ports from their digitised global peers. Its value is grounded in two reinforcing mechanisms: the improvement of operational performance through AI–IoT integration under favourable conditions, and the protection of system resilience through

cybersecurity as the safeguarding subsystem. Nonetheless, the realisation of this value is constrained by unreliable power and telecommunications infrastructure, shortages of skilled human capital, fragmented data and rising cyber risk. The central lesson is that the smart port is a system: its benefits accrue not from any single technology but from the secure integration of all three, supported by the infrastructure, skills and strategy that make integration work.

In an era when smart ports are transitioning worldwide from pilots to operational reality, Nigeria's window to secure regional leadership in digital logistics is open but not indefinite. The quantitative evidence presented here should strengthen the resolve of policymakers and operators to pursue an integrated, secure and well-resourced path to smart port transformation, converting a long-standing source of economic friction into a foundation of competitiveness and growth.

10. Recommendations

On the basis of the findings, the study makes the following recommendations:

1. The Nigerian Ports Authority and government should develop and implement a national smart-port strategy that advances AI, IoT and cybersecurity integration in tandem, rolling out pilot projects and scaling successful models across all port locations.
2. Government and operators should prioritise the enabling infrastructure on which smart ports depend, particularly reliable electricity supply and robust telecommunications connectivity, since digital port systems cannot function effectively without them.
3. Port stakeholders should invest in cybersecurity as an integral component of digitalisation rather than an afterthought, deploying threat protection, data security and incident-response capabilities to safeguard automated terminals and sensitive trade data.
4. Government, operators and academic institutions should jointly invest in human-capital development, training workers in cybersecurity, data analytics, predictive maintenance and related Industry 4.0 skills identified as the critical gap in smart port transformation.
5. Port authorities should drive data standardisation and interoperability across agencies through initiatives such as the National Single Window and port community systems, since fragmented data and limited interoperability are principal sources of current inefficiency.
6. Future research should employ longitudinal designs and objective operational data such as measured dwell and turnaround times, and should extend the analysis to Nigeria's eastern ports to assess the generalisability of these findings.

REFERENCES

Envision Enterprise Solutions. (2025). *The future of maritime logistics: How smart ports are shaping global trade in 2025*. Retrieved from <https://www.envisionesl.com/blog/>

- Free Trade Nigeria. (2022). *Why Nigeria should digitize its ports operation quickly*. Retrieved from <https://freetradenigeria.com/>
- Guardian Nigeria. (2026). *How weak infrastructure threatens Nigeria's smart port transition*. The Guardian (Nigeria), Maritime.
- IBM. (2024). *Cost of a data breach report 2024*. IBM Security.
- Interesting Engineering. (2025). *How AI, IoT, and automation are transforming smart ports*. Retrieved from <https://interestingengineering.com/innovation/ai-iot-automation-smart-ports>
- International Union of Marine Insurance (IUMI). (2025). *Smart ports: A technology-driven transformation*. IUMI Newsletter, December 2025.
- MarketsandMarkets. (2025). *Smart port market report 2025–2030, by technology and geography*. MarketsandMarkets Research.
- Nwogute, U., Dahiru, S. I., & Aruwa, S. A. S. (2026). Effect of port digitization on the logistics performance of maritime supply chains in Nigerian Ports Authority Apapa and Tin Can Island ports. *International Journal of Research and Innovation in Social Science*, 10(1). <https://doi.org/10.47772/IJRISS.2026.10100458>
- Ship-Technology. (2021). *Nigeria aims for digitalised port operations by 2025*. Retrieved from <https://www.ship-technology.com/news/>
- ThisDay. (2025). *How Nigeria's 5G-enabled smart port is transforming Lagos into West Africa's logistics powerhouse*. ThisDayLive.
- Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.
- UNIS. (2025). *All other Nigeria ports: Nigeria container hub*. Retrieved from <https://www.unisco.com/international-ports/>
- von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. George Braziller.
- Walmart, A., Noel, D., & Phillips, J. (2024). *The role of IoT and AI in enhancing Ghana's port logistics and security*. ResearchGate.